UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/592,322	06/13/2000	Slawomir K. Ilnicki	10992668-1	7389

22879 7590 07/15/2004

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
REVAK, CHRISTOPHER A	

ART UNIT	PAPER NUMBER
2131	5

DATE MAILED: 07/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/592,322	ILNICKI ET AL.
	Examiner	Art Unit
	Christopher A. Revak	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 April 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments with respect to claims 1-26 have been considered but are moot in view of the new ground(s) of rejection.

The applicant has amended the claims, wherein the examiner has found the added limitations still taught by the teachings of Baker et al. Please refer to the rejection as is recited below.

The examiner has withdrawn the objections to the specification and claims.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 23 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In claim 22, it is recited of "without requiring a trusted intermediate party" and claim 23 recites that the trusted intermediate party is further limiting to either a trusted node, a trusted server, or secure channel. Since claim 22 recites of the trusted intermediate party is not required, the language of claim 23 is ambiguous since the trusted intermediate party as being either a trusted node, a trusted server, or secure channel is not required.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-5,11,14-22,25, and 26 are rejected under 35 U.S.C. 102(e) as being anticipated by Baker et al.

In regards to claim 1, Baker teaches a method for securely transferring data (i.e. a tool for enabling customers to manage their telecommunications assets, quickly and securely) (col. 5, line 29-31) between an agent (i.e. downloadable application object) (col. 5, line 60-61) and an application server (i.e. MCI Intranet Application server) through a non-secure node (i.e. Web Server)(col. 6, lines 35-41) comprising:

(a) establishing a session key (col. 17, line 10-11) between the agent and the application server by utilizing a public key of the application server (col. 11, lines 37-38); wherein the public key ofthe application server is embedded in the agent (i.e. it generates a "cookie" which is a uniqueserver-generated key that is sent to the client along with each reply to a HTTPS request)(col. 9,lines 10-12) (The Examiner infers from the above that the cookie is also sent with/embedded the downloadable agent) wherein

the message manager (agent) is responsible for generating the session key (col. 16, lines 11-14); and

(b) establishing an end-to-end secure connection between the agent and the application server by using the session key (i.e. the client holds the cookie and returns it to the server as part of each subsequent HTTPS request) (col. 9, lines 12-14) and by establishing a communication link between the application server and the non-secure node by using a relay module (i.e. the communications from the client and back-end via the web server are conducted using the common gateway interface [CGI]. Requests from the client are typically first targeted at a CGI program, which then relays the request to the appropriate proxy process. Results are returned from back-end processes to the requesting client in the same manner.) (col. 15, lines 13-20).

In regards to claim 2, Baker teaches wherein establishing a communication link between the application server and the non-secure node by using a relay module comprises:

dynamically instantiating, by the application server (col. 10, lines 22-34 and col. 18, lines 13-25) the relay module (i.e. the HTTP service manager spawns a process to run an instance of the message manager) (col. 16, lines 3-5) having a first port for communicating with the application server (message transactions are sent to the proxy server over a new connection by opening a new TCP socket to the proxy server)(col. 16, lines 20-22) and a second port for communicating with the agent (i.e. both input and output streams are created by the message manager to receive message data from the

client and to reply back to the client) (col. 16, line 9-11), the relay module listening on a first predetermined port number on the first port and a second predetermined port number on the second port; and the application server connecting to the first port of the relay module to establish a connection therewith (i.e. after one of the DMZ Web servers decrypts and verifies the user session, it forwards the message through a firewall over a TCP/IP connection to the dispatch server on a new TCP socket while the original socket from the browser is blocking, waiting for a response. The dispatch server unwraps an outer protocol layer of the message from the DMZ services cluster, and re-encrypts the message with symmetric encryption and forwards the message to an appropriate application proxy via a third TCP/IP socket. While waiting for the proxy response all three of the sockets block on a receive.) (col. 9, lines 22-33). The Examiner interprets "waiting for a response" to be equivalent to listening for a connection.

In regards to claim 3, Baker teaches wherein establishing a communication link between the application server and the agent through a relay module further comprises: pushing data encrypted by the established session key from the agent to the application server over the end-to-end secure connection (i.e. the web server decrypts the message and wraps the message with the user's information, including environment variables and a server-generated session identifier (id). The message is then encrypted and forwarded to the CMID, or alternately, as will be described below, to the proxy server component of the CMID) (col. 16, lines 36-42).

In regards to claim 4, Baker teaches wherein establishing a communication link between the application server and the agent through a relay module further comprises: pulling data (i.e. the HTTP service manager downloads the HTML files and Java applets to the client upon request via the HTTPS port) (col. 16, lines 31-33) encrypted by the session key from the application server over the end-to-end secure connection to the agent (i.e. typically, communications to and from the client take place over hyper-text transfer protocol secure (HTTPS) which uses the hyper-text transfer protocol (HTPP) over a secure socket layer (SSL) encrypted channel (col. 16, lines 25-28).

In regards to claim 5, Baker teaches establishing a shared secret key between the application server and the agent for encrypting and decrypting data sent there between (i.e. after one of the DMZ Web servers decrypts and verifies the user session, it forwards the message through a firewall over a TCP/IP connection to the dispatch server on a new TCP socket while the original socket form the browser is blocking, waiting for a response. The dispatch server unwraps an outer protocol layer of the message from the DMZ services cluster and re-encrypts the message with symmetric encryption and forwards the message to an appropriate application proxy via a third TCP/IP socket (col. 9, lines 22-31). The Examiner infers that in order to use symmetric encryption a shared key must have been established.

In regards to claim 11, Baker teaches the method of securely transferring data (i.e. a tool for enabling customers to manage their telecommunications assets, quickly and

securely) (col. 5, line 29-31) between an application server (i.e. MCI Intranet Application server) (col. 6, line 39-40) and an agent of the application server (i.e. downloadable application object) (col. 5, line 60-61) through a non-secure environment having a web-server (i.e. a Demilitarized Zone [DMZ] comprising Web Servers) (col. 6, line 37-38) and the agent, the method comprising:

a) a user accessing the web-server to download the agent therefrom (col. 14, line 7-10); wherein the agent includes a public key of the application server (i.e. a "cookie" which is a unique server-generated key that is sent to the client along with each reply to a HTTPS request)(col. 9, line 10-12) (the nMCI Interact system security infrastructure includes public key encryption) (col. 11, lines 34-38);

b) the agent deriving a shared session key with the application server by using the public key of the application server (i.e. the client is provided a "session id" which is a unique server-generated key. The session table maintains a "session key table" which maps these keys to the associated session) (col. 17, lines 7-11), the shared session key for use in encrypting and decrypting data to be transferred between the agent and the application server (i.e. each transaction from a client is sent to the web server in the form of a logical message that has been encrypted) (col. 16, lines 34-36) (see also col. 8, lines 29-32; and col. 9, lines 22-25);

c) the application server establishing a connection to the web-server (i.e. after one of the DMZ Web servers decrypts and verifies the user session, it forwards the message through a firewall over a TCP/IP connection to the dispatch server) (col. 9, lines 22-25): and

d) the agent contacting the web server by using a first protocol (i.e. SSL) to send data encrypted by the session key to the application server over the connection between the web-server and the application server (i.e. objects will communicate the data by establishing a secure TCP messaging session with one of the DMZ network MCI Interact Web servers via an Internet secure communication path established, preferably, with a secure sockets SSL version of HTTPS) (col. 8, lines 24-29).

In regards to claim 14, Baker teaches wherein the first protocol is one HTTP and HTTP/SSL (i.e. the nMCI Interact system is implemented with a secure version of HTTP such as S-HTTP or HTTPS, and preferably utilizes the SSL implementation of HTTPS) (col. 9, lines 2-5).

In regards to claim 15, Baker teaches a secure data transfer system (i.e. a tool for enabling customers to manage their telecommunications assets, quickly and securely) (col. 5, line 29-31) for connecting a non-secure node (i.e. Web Server) (col. 6, line 38) to an application server (i.e. MCI Intranet Application server) (col. 6, line 39-40) behind a firewall (i.e. The DMZ is generally bounded by two firewalls) (col. 14, line 15) comprising:

a) a web-server in the non-secure node (figure 2, element 24):

b) a relay (i.e. message manager) in the non-secure node that is dynamically instantiated by the application server (i.e. the HTTP service manager spawns a process to run an instance of the message manager) (col. 16, lines 3-5), the relay being

configured by the application server (col. 10, lines 22-34 and col. 18, lines 13-25) having a first port for listening for a connection from the application server;

wherein the application server connects to the relay on the first port and reads data from the first port (i.e. message data is passed to the message manager by opening an input stream and an output stream within the thread) (col. 16, lines 48-50). Baker also adds that "results are returned from back-end processes to the requesting client in the same manner" (col. 15, lines 18-20). The Examiner infers from the above that the method of instantiating the relay and connecting to the port can hence be equally performed from the web-server or from the application server.

In regards to claim 16, Baker teaches the secure data transfer system of claim 15 as discussed above, further comprising:

a) an instantiation module (i.e. HTTP service manager) for instantiating the relay module (col. 16, lines 3-5).

b) the relay does not initiate the connection with the application server but waits for the application server to establish the connection (col. 10, lines 22-34).

In regards to claims 17 and 22, Baker teaches a secure data transfer system for establishing an end-to-end secure connection (i.e. a tool for enabling customers to manage their telecommunications assets, quickly and securely) (col. 5, line 29-31) between an agent (i.e. downloadable application object) (col. 5, line 60-61) and an application server behind a firewall through a non-secure node comprising:

a) a web-server residing in the non-secure node (i.e. Call Manager Web Server) (figure 2, element 632), the web-server having the agent that includes a public key of the application server (i.e. a "cookie" which is a unique server-generated key that is sent to the client along with each reply to a HTTPS request) (col. 9, line 10-12);

b) a browser in communication with the web-server for downloading the agent from the web-server (figure 2, element 20);

c) a secure transfer module (i.e. CGI program) residing in the non-secure node (col. 15,lines 16-18); and

d) an application server (i.e. Call Manager Server) (figure 2, element 640) in a secure zone (i.e. MCI Intranet) (figure 2, element 30) for initiating a connection to the web-server via the secure transfer module.

It is noted by the examiner that the teachings of Baker et al do not disclose of a "trusted intermediate party" for transferring data between a browser through a relay module to an application server.

In regards to claim 18, Baker teaches the secure data transfer system of claim 17, as discussed above, wherein the secure transfer module further comprises:

c1) a relay module (i.e. a CGI program) (col. 15, lines 16-18) for listening to a first port and a second port (i.e. both input and output streams are created by the message manager to receive message data from the client and to reply back to the client) (col. 16, lines 9-11);

c2) an instantiation module for executing the relay module in response to a command from the application server (i.e. the HTTP service manager spawns a process to run an instance of the message manager) (col. 16, lines 3-5). Baker adds that "message data is passed to the message manager by opening an input stream and an output stream within the thread" (col. 16,lines 48-50). Baker also adds that "results are returned from back-end processes to the requesting client in the same manner" (col. 15, lines 18-20). The Examiner infers from the above that the method of instantiating the relay and connecting to the port can hence be equally performed from the web-server or from the application server;

c3) a forwarding module (i.e. a middle tier transaction handler) (col. 15, lines 38-41) for transferring data from the agent to the relay module (i.e. HTTP CGI)(col. 15, line 41) in response to a command from the agent; and wherein the relay module listens to the first port for a connection by the application server and listens to the second port for a connection by the forwarding module (i.e. after one of the DMZ Web servers decrypts and verifies the user session, it forwards the message through a firewall over a TCP/IP connection to the dispatch server on a new TCP socket while the original socket from the browser is blocking, waiting for a response. The dispatch server unwraps an outer protocol layer of the message from the DMZ services cluster, and re-encrypts the message with symmetric encryption and forwards the message to an appropriate application proxy via a third TCP/IP socket. While waiting for the proxy response all three of the sockets block on a receive.) (col. 9, lines 22-33). The Examiner interprets "waiting for a response" to be equivalent to listening for a connection.

In regards to claim 19, Baker teaches the secure data transfer system of claim 16, as discussed above, wherein the non-secure node is a web-server (figure 2, element 24).

As per claims 20 and 26, Baker et al discloses of transferring data between the agent and relay module via an unsecure communication link (col. 5, lines 60-61, col. 6, lines 35-41, and col. 15, lines 16-18).

As per claim 21, Baker et al recites of transferring data between the agent and the web-server via an unsecure communication link (col. 5, lines 29-31,60-61 and col. 6, lines 35-41).

As per claim 25, Baker discloses of an agent measuring time required to load data into a browser (col. 10, lines 35-40).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 6-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baker et al in view of Curry et al.

In regards to claim 6, Baker teaches the method of claim 5 as discussed above.

Baker, however, does not teach encrypting the shared secret key with the public key of the application server to generate an encrypted shared key; sending the encrypted shared secret key to the application server; and decrypting the shared secret key with the private key of the application server.

Curry discloses a similar method, apparatus and system for transferring money or its equivalent electronically. In particular, in an electronic module based system, the module can be configured to provide at least secure data transfers or to authorize monetary transactions (col. 1, lines 25-28).

Curry teaches encrypting the shared secret key with the public key of the application server to generate an encrypted shared key; sending the encrypted shared secret key to the application server; and decrypting the shared secret key with the private key of the application server (i.e. when someone wishes to send private e-mail to this user, he generates a random IDEA encryption key and encrypts the entire message with the IDEA encryption algorithm. He then encrypts the IDEA key itself using the public key provided by the intended recipient. He e-mails both the message encrypted with IDEA and the IDEA key encrypted with the user's public key to the user. No one that sees this transmission can read it except the intended recipient because the message is encrypted with IDEA and the IDEA key is encrypted with the intended recipient's public key. The recipient's computer contains the corresponding private key, and hence can decrypt the IDEA key and use the decrypted IDEA key to decrypt the message) (col. 15, lines 31-43).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Baker with the teachings of Curry to include encrypting the shared secret key with the public key of the application server to generate an encrypted shared key; sending the encrypted shared secret key to the application server; and decrypting the shared secret key with the private key of the application server with the motivation of providing security from those who might try to read the user's email (i.e. messages) remotely (Curry, col. 5, lines 44-45).

In regards to claim 7, Baker teaches to method of claim 5 as discussed above.

Baker, however, does not teach wherein establishing a shared secret key between the application server and the agent utilizes a key transfer protocol.

Curry teaches wherein establishing a shared secret key between the application server and the agent utilizes a key transfer protocol (i.e. he makes his public key widely available by putting it in the signature block of all his e-mail messages and arranging to have it posted in publicly accessible directories of P.G.P. public keys) (col. 5, lines 26-29).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Baker with the teachings of Curry to include wherein establishing a shared secret key between the application server and the agent utilizes a key transfer protocol with the motivation of providing security from those who might try to read the user's email (i.e. messages) remotely (Curry, col. 5, lines 44-45).

In regards to claim 8, the combination of Baker and Curry teaches the method of claim 7 as discussed above.

The combination as discussed above does not teach wherein the key transfer protocol is the Rivest, Shamir, Adleman (RSA) public key algorithm.

Curry teaches wherein the key transfer protocol is the Rivest, Shamir, Adleman (RSA) public key algorithm (i.e. to use P.G.P. a user generates a complete RSA key set containing both a public and private component) (col. 5, lines 24-26).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to further modify the teachings of Baker and Curry with the teachings of Curry to include wherein the key transfer protocol is the Rivest, Shamir, Adleman (RSA) public key algorithm with the motivation of providing security from those who might try to read the user's email (i.e. messages) remotely (see Curry, col. 5, lines 44-45).

8. Claims 9 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baker et al in view of Boyle et al.

In regards to claims 9 and 10, Baker teaches the method of claim 5 as discussed above.

Baker, however, does not teach wherein establishing a shared secret key

between the application server and the agent for encrypting and decrypting data sent there between utilizes a key agreement protocol, and wherein the key agreement protocol is the Diffie-Hellman (DH) public key algorithm.

Boyle discloses a method for processing data pushed over a network from a data source or sources to a data destination or destinations via a computer system intermediate between the source or sources and the destination or destinations, wherein the intermediate computer system communicates with the source or sources and destination or destinations over the network (col. 1, lines 54-60).

Boyle teaches wherein establishing a shared secret key between the application server and the agent for encrypting and decrypting data sent there between utilizes a key agreement protocol, and wherein the key agreement protocol is the Diffie-Hellman (DH) public key algorithm (i.e. the Diffie-Hellman key exchange protocol is used in the process to securely distribute the shared secret key to the device after appropriate authentication) (col. 30, lines 63-66).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teachings of Baker with the teachings of Boyle to include wherein establishing a shared secret key between the application server and the agent for encrypting and decrypting data sent therebetween utilizes a key agreement protocol, and wherein the key agreement protocol is the Diffie-Hellman (DH) public key algorithm with the motivation to reduce the use of network resources and make it faster for the client to access data from the server (see Boyle, col. 2, line 67, and col. 3, line 1).

9. Claims 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Baker et al in view of Bradley et al.

In regards to claim 12, Baker teaches the method of claim 11 as discussed above. Baker further teaches wherein the application server establishing a connection to the Web-server further comprises

c1) the application server dynamically instantiating a relay module (i.e. the HTTP service manager spawns a process to run an instance of the message manager) (col. 16, lines 3-5). Baker adds that "message data is passed to the message manager by opening an input stream and an output stream within the thread" (col. 16, lines 48-50). Baker also adds that "results are returned from back-end processes to the requesting client in the same manner" (col. 15, lines 18-20). The Examiner infers from the above that the method of instantiating the relay and connecting to the port can hence be equally performed from the web-server or from the application server;

c2) the application server connecting to the relay module on a first predetermined port (i.e. message transactions are sent to the proxy server over a new connection by opening a new TCP socket to the proxy server) (col. 16, lines 20-22);

c3) the application server reading data from the relay module through the connection on the first predetermined port (i.e. the CGI program then relays the request to the appropriate proxy server) (col. 15, lines 17-18).

Baker does not teach sending a URL associated with the relay module to the

web-server, the URL specifying a first predetermined port for communication between the web-server and the relay module.

Bradley teaches sending a URL associated with the relay module to the web-server, the URL specifying a first predetermined port for communication between the web-server and the relay module (i.e. In one embodiment, the connection information specifies the types of context as well as the format in which the context information should be sent to the third party application. This is also known as Contextual Calling. For example, the user may select information items from a set of known contextual items, including device name, IP address, device interface, port address, security levels. The user may select the manner in which the contextual item is passed as a key/value pair to a 3rd-party application URL.) (col. 20, lines 29-37).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teachings of Baker with the teachings of Bradley to include sending a URL associated with the relay module to the web-server, the URL specifying a first predetermined port for communication between the web-server and the relay module with the motivation to produce a simple and inexpensive method or mechanism to automatically and correctly link external application to enterprise network managements systems (see Bradley, col. 2, lines 17-20).

10. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Baker et al in view of Bradley et al in further view of Curry et al.

In regards to claim 13, the combination of Baker and Bradley teaches the method of claim 12 as discussed above.

The combination, however, does not teach establishing a connection to the web-server further comprising:

d1) the agent encrypting the session key with the public key of the application server:

d2) the agent collecting data;

d3) the agent encrypting the collected data using the session key;

d4) sending the encrypted session key and encrypted measured data to the application server by using a forwarding module that connects to a second predetermined port of the relay module.

Curry discloses a similar method, apparatus and system for transferring money or its equivalent electronically. In particular, in an electronic module based system, the module can be configured to provide at least secure data transfers or to authorize monetary transactions (col. 1, lines 25-28).

Curry teaches establishing a connection to the web-server further comprising:

d1) the agent encrypting the session key with the public key of the application server (i.e. he then encrypts the IDEA key itself using the public key provide by the intended recipient) (col. 5, lines 34-36);

d2) the agent collecting data (i.e. sending private e-email) (col. 5, line 32);

d3) the agent encrypting the collected data using the session key (i.e. the message is encrypted with IDEA) (cot. 5, lines 39-40);

d4) sending the encrypted session key and encrypted measured data to the application server by using a forwarding module that connects to a second predetermined port of the relay module (He e-mails both the message encrypted with IDEA and the IDEA key encrypted with the user's public key to the user) (cot. 5, lines 36-38).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Baker and Bradley with the teachings of Curry to include establishing a connection to the web-server further comprising:

d1) the agent encrypting the session key with the public key of the application server:

d2) the agent collecting data;

d3) the agent encrypting the collected data using the session key;

d4) sending the encrypted session key and encrypted measured data to the application server by using a forwarding module that connects to a second predetermined port of the relay module, with the motivation of providing security from those who might try to read the user's email (i.e. messages) remotely (Curry, cot. 5, lines 44-45).

11. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Baker et al in view of Curry et al.

Baker et al fails to disclose of an agent collecting data.

Curry discloses a similar method, apparatus and system for transferring money or its equivalent electronically. In particular, in an electronic module based system, the module can be configured to provide at least secure data transfers or to authorize monetary transactions (col. 1, lines 25-28).

Curry teaches establishing a connection to the web-server further comprising:

d1) the agent encrypting the session key with the public key of the application server (i.e. he then encrypts the IDEA key itself using the public key provide by the intended recipient) (col. 5, lines 34-36);

d2) the agent collecting data (i.e. sending private e-email) (col. 5, line 32);

d3) the agent encrypting the collected data using the session key (i.e. the message is encrypted with IDEA) (cot. 5, lines 39-40);

d4) sending the encrypted session key and encrypted measured data to the application server by using a forwarding module that connects to a second predetermined port of the relay module (He e-mails both the message encrypted with IDEA and the IDEA key encrypted with the user's public key to the user) (cot. 5, lines 36-38).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Baker and Bradley with the teachings of Curry to include establishing a connection to the web-server further comprising:

d1) the agent encrypting the session key with the public key of the application server:

d2) the agent collecting data;

d3) the agent encrypting the collected data using the session key;

d4) sending the encrypted session key and encrypted measured data to the application server by using a forwarding module that connects to a second predetermined port of the relay module, with the motivation of providing security from those who might try to read the user's email (i.e. messages) remotely (Curry, cot. 5, lines 44-45).

Conclusion

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 703-305-1843. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CR

July 7, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100